

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-184173
(43)Date of publication of application : 30.06.2000

(51)Int.CI.

H04N 1/387
G06T 1/00
G09C 5/00
H04L 9/32
H04N 1/44

(21)Application number : 10-352619

(71)Applicant : CANON INC

(22)Date of filing : 11.12.1998

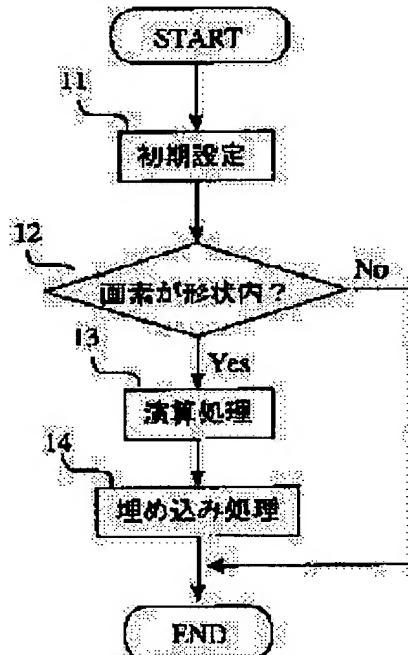
(72)Inventor : YOSHIDA ATSUSHI
IWAMURA KEIICHI

(54) METHOD AND DEVICE FOR PICTURE PROCESSING, METHOD AND SYSTEM FOR PICTURE DELIVERY, AND COMPUTER READABLE STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To embed a picture with a visual digital watermark which has a high security and is easily restored.

SOLUTION: An original picture consisting of plural picture elements consisting of picture element positions and picture element values, watermark picture shape information consisting of the picture element position indicating the shape of a picture to be embedded with, and a prescribed serial bit sequence expressed with binary numbers as a sequence are set in a initial state processing 11. In processing 12, the picture element position of a picture element constituting the original picture and watermark picture shape information are compared with each other. If they coincide with each other, this picture element position information is sent to processing 13; and if they don't coincide, the processing of this picture element is terminated. In the processing 13, the operation processing using picture element values (the whole or a part) in designated picture element positions of the original picture and prescribed bit (or a bit string) as the padding sequence is performed to generate a picture padded with the visual digital watermark.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-184173

(P2000-184173A)

(43)公開日 平成12年6月30日 (2000.6.30)

(51) Int.Cl. ¹	識別記号	F I	マークト ² (参考)
H 04 N 1/387		H 04 N 1/387	5 B 0 5 7
G 06 T 1/00		G 09 C 5/00	5 C 0 7 5
G 09 C 5/00		H 04 N 1/44	5 C 0 7 6
H 04 L 9/32		G 06 F 15/68	B 5 J 1 0 4
H 04 N 1/44		H 04 L 9/00	6 7 5 D

審査請求 未請求 請求項の数21 OL (全9頁)

(21)出願番号	特願平10-352619	(71)出願人	000001007 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
(22)出願日	平成10年12月11日 (1998.12.11)	(72)発明者	吉田 淳 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内
		(72)発明者	岩村 恵市 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内
		(74)代理人	100090273 弁理士 國分 孝悦

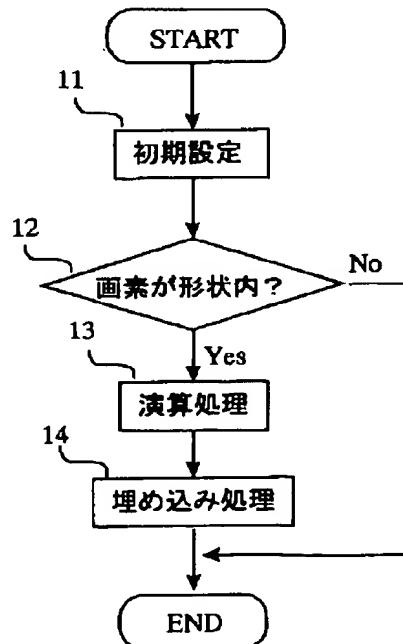
最終頁に続く

(54)【発明の名称】 画像処理方法、装置、画像配付方法、システム及びコンピュータ読み取り可能な記憶媒体

(57)【要約】

【課題】 セキュリティの高い、かつ復元の容易な可視型の電子透かしを画像に埋め込む。

【解決手段】 処理1 1の初期状態で、画素位置と画素値で構成される複数の画素からなる原画像と、埋め込む画像の形状を示す画素位置からなる透かし画像形状情報と、埋め込み系列としての2進数で表現される所定のシリアルビット系列を設定する。処理1 2では、原画像を構成する画素の画素位置と透かし画像形状情報を比較し、一致したときはその画素についての処理を終了する。処理1 3では、原画像の指定された画素位置の画素値(全部又は一部)と、上記埋め込み系列としての所定のビット(又はビット列)を用いた演算処理を行うことにより、可視型の電子透かしが埋め込まれた画像を作成する。



し画像形状情報及び埋め込み系列を入力する処理と、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と、上記埋め込み系列との演算を行うことにより上記電子透かしを解除する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項21】 原画像、透かし画像形状情報及び埋め込み系列を入力する処理と、

上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する処理と、

上記作成された電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列をユーザに配付する処理と、

上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と、上記埋め込み系列との逆演算を行うことにより、上記電子透かしを解除する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、画像の著作権保護、画像の改竄防止等のために、画像に電子透かし等の目視しにくい情報を埋め込むための方法、装置、電子透かしが埋め込まれた画像の電子透かしを解除するための方法、装置、サーバにおいて電子透かしが埋め込まれた画像を作成して、ユーザに配付し、ユーザにおいて電子透かしを解除する画像配付方法、システム及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【0002】

【従来の技術】 画像をデジタルデータとして扱うデジタル画像には、従来のアナログ画像と比較して、コンピュータ等によって画質を劣化すること無く簡単にコピーでき、通信回線を通じて電送することができるという特徴がある。このような特徴により、デジタル画像は安易に不正コピーされ再配布されてきた。これを防ぐための方法の一つとして電子透かしと呼ばれる手法がある。電子透かしには、大きく分類して著作権情報、ユーザ情報等の透かし情報を目に見えない形で埋め込む不可視型と、画像上に著作権を保有する会社のロゴ等の透かし画像を目に見える形で形成する可視型とがある。

【0003】 不可視型の電子透かしでは、透かし情報が埋め込まれているということが、埋め込み画像を一見しただけでは認識できない。このため、透かし情報の削除は行われにくいものの、不正コピー、不正配布は可視型に比べ行われ易い。但し、例えデジタル画像が不正にコピー又は配布された場合であっても、そのデジタル画像中には透かし情報が残っているので、透かし情報として

埋め込まれたユーザID等により、不正ユーザを特定することができる。

【0004】 不可視型の電子透かしの代表的なものとして、入力画像に対し高速フーリエ変換、離散コサイン変換、ウェーブレット変換等の周波数変換を行い、周波数領域に透かし情報を加えた後、逆周波数変換を行うことにより埋め込みを行う手法がある。上記高速フーリエ変換による手法では、入力画像は、PN系列を加えられて拡散された後、ブロックに分割される。ブロック毎にフーリエ変換が施され、1ブロックに1ビットの透かし情報が埋め込まれる。透かし情報が埋め込まれたブロックは逆フーリエ変換が施され、再び最初と同じPN系列が加えられて合成画像となる。これは、大西、岡、松井、"PN系列による画像への透かし署名法" 1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26Bに詳しい。

【0005】 上記離散コサイン変換による手法は、ブロックに分割し、ブロック毎に離散コサイン変換をする。1ブロックに1ビットの情報を埋め込んだ後、逆変換をして合成画像を生成する。これは、中村、小川、高嶋"ディジタル画像の著作権保護のための周波数領域における電子透かし方式" 1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26Aに詳しい。

【0006】 上記ウェーブレット変換による手法は、入力画像をブロック分割する必要のない手法である。これは、石塚、酒井、櫻井、"ウェーブレット変換を用いた電子すかし技術の安全性と信頼性に関する実験的考察" 1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26Dに詳しい。

【0007】 また、画素の色相、明度等に演算を施して電子透かしを埋め込む手法 (Digimarc社、米国特許5,636,292号等) もある。

【0008】 一方、上記可視型電子透かしでは、透かし情報は、デジタル画像上に目で見える形で書き込まれているので、そのままでは利用し辛く、不正コピーや不正配布を思いとどまらせる効果がある。可視型の電子透かしの埋め込み方法として、従来、著作権所有者のロゴ等の著作情報を表した画像の画素値を、原画像の画素値と置き換えることにより、著作情報を原画像に埋め込むという手法がよく用いられてきた。この手法の欠点としては、原画像の画素値が失われるため、原画像を復元できないことが挙げられる。

【0009】 上述したように、従来の可視型電子透かし埋め込み手法においては、原画像を復元する方法は用意されておらず、正規の原画像を得たい場合は、原画像の全てを再取得する必要があった。

【0010】 また、電子透かしの他にデジタル画像の著作権を保護するための手法として、次のような方法が特開平9-233455号公報及び米国特許5,491,

【特許請求の範囲】

【請求項1】 原画像、透かし画像形状情報及び埋め込み系列を入力とし、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより、情報が埋め込まれた画像を作成するようにしたことを特徴とする画像処理方法。

【請求項2】 上記演算に共通鍵暗号方式による暗号化処理を用いることを特徴とする請求項1記載の画像処理方法。

【請求項3】 上記演算に公開鍵暗号方式による暗号化処理を用いることを特徴とする請求項1記載の画像処理方法。

【請求項4】 上記原画像が、不可視型電子透かしが埋め込まれている画像であることを特徴とする請求項1記載の画像処理方法。

【請求項5】 上記電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列を出力することを特徴とする請求項1記載の画像処理方法。

【請求項6】 原画像、透かし画像形状情報、及び埋め込み系列を入力する入力手段と、

上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する演算手段とを設けたことを特徴とする画像処理装置。

【請求項7】 上記演算に共通鍵暗号方式による暗号化処理を用いることを特徴とする請求項6記載の画像処理装置。

【請求項8】 上記演算に公開鍵暗号方式による暗号化処理を用いることを特徴とする請求項6記載の画像処理装置。

【請求項9】 上記原画像が、不可視型電子透かしが埋め込まれている画像であることを特徴とする請求項6記載の画像処理装置。

【請求項10】 上記電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列を出力する出力手段を設けたことを特徴とする請求項6記載の画像処理装置。

【請求項11】 電子透かしが埋め込まれた画像、透かし画像形状情報及び埋め込み系列を入力し、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と、上記埋め込み系列との演算を行うことにより上記電子透かしを解除するようにしたことを特徴とする画像処理方法。

【請求項12】 上記演算に共通鍵暗号方式による暗号化処理を用いることを特徴とする請求項11記載の画像処理方法。

【請求項13】 上記演算に公開鍵暗号方式による暗号化処理を用いることを特徴とする請求項11記載の画像

処理方法。

【請求項14】 サーバにおいて、原画像、透かし画像形状情報、及び埋め込み系列を入力とし、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより、電子透かしが埋め込まれた画像を作成し、この電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列をユーザに配付し、上記ユーザにおいて、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と上記埋め込み系列との逆演算を行うことにより、上記電子透かしを解除するようにしたことを特徴とする画像配付方法。

【請求項15】 電子透かしが埋め込まれた画像、透かし画像形状情報及び埋め込み系列を入力する入力手段と、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と、上記埋め込み系列との演算を行うことにより上記電子透かしを解除する演算手段を設けたことを特徴とする画像処理装置。

【請求項16】 上記演算に共通鍵暗号方式による暗号化処理を用いることを特徴とする請求項15記載の画像処理装置。

【請求項17】 上記演算に公開鍵暗号方式による暗号化処理を用いることを特徴とする請求項15記載の画像処理装置。

【請求項18】 原画像、透かし画像形状情報及び埋め込み系列を入力する入力手段と、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する演算手段とを有するサーバと、

上記電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列をユーザに配付する配付手段と、

上記電子透かしが埋め込まれた画像、透かし画像形状情報及び埋め込み系列を入力する入力手段と、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と上記埋め込み系列との逆演算を行うことにより、上記電子透かしを解除する演算手段とを有するユーザとを備えたことを特徴とする画像配付システム。

【請求項19】 原画像、透かし画像形状情報、及び埋め込み系列を入力する処理と、

上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項20】 電子透かしが埋め込まれた画像、透か

563号で提案されている。即ち、画像符号化器の直後にスクリンブル装置を接続して、符号化された入力画像情報に対してスクリンブルを行い、受信者施設へ送る。受信者施設では、画像復号器の直前にスクリンブル解除装置を接続して、スクリンブルの解除を行うものである。

【0011】この手法では、原画像の全てあるいは一部の画素について、ある鍵に依存した形でスクリンブルされるが、スクリンブルされた全ての画素値は、画像上に画素を取り出した部分に埋め戻されるので、鍵を手に入れることによりスクリンブルを解除することが可能となっている。しかし、このように画像にスクリンブルをかける方法では、画像の不正利用は防げるものの、著作権情報等の情報を画像上に埋め込むことはできず、画像とは別に著作権情報を配布する必要があった。

【0012】

【発明が解決しようとする課題】上記従来例で説明したように、従来の不可視型の電子透かしを著作権保護の目的で使用した場合、不正再配布が行われ易いという問題があった。また、可視型の電子透かしにおいては、原画像を復元する方法が用意されていないという問題があった。また、スクリンブルによる方法では、画像の不正利用は防げるものの、著作権情報を画像上に埋め込むことができず、画像とは別に著作権情報を配布する必要があった。上記のような問題により、どの方法も著作権保護の目的のために使用するには十分なものではなかった。

【0013】本発明は、上記の問題を解決するために成されたもので、著作権保護を十分に行うことができるようすることを目的としている。

【0014】

【課題を解決するための手段】上記の目的を達成するために、本発明による画像処理方法においては、原画像、透かし画像形状情報、及び埋め込み系列を入力とし、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより、情報が埋め込まれた画像を作成するようとしている。

【0015】また、本発明による画像処理装置においては、原画像、透かし画像形状情報、及び埋め込み系列を入力する入力手段と、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する演算手段とを設けてい

る。【0016】また、本発明による他の画像処理方法においては、電子透かしが埋め込まれた画像、透かし画像形状情報、及び埋め込み系列を入力とし、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と、上記埋め込み系列との演算を行うことにより、上記電子透かしを解除

するようとしている。

【0017】また、本発明による画像配付方法においては、サーバにおいて、原画像、透かし画像形状情報、及び埋め込み系列を入力とし、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより、電子透かしが埋め込まれた画像を作成し、上記電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列をユーザに配付し、上記ユーザにおいて、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と上記埋め込み系列との演算を行うことにより上記電子透かしを解除するようとしている。

【0018】また、本発明による他の画像処理装置においては、電子透かしが埋め込まれた画像、透かし画像形状情報、及び埋め込み系列を入力する入力手段と、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と、上記埋め込み系列との演算を行うことにより上記電子透かしを解除する演算手段とを設けている。

【0019】また、本発明による画像配付システムにおいては、原画像、透かし画像形状情報及び埋め込み系列を入力する入力手段と、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する演算手段とを有するサーバと、上記電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列をユーザに配付する配付手段と、上記電子透かしが埋め込まれた画像、透かし画像形状情報及び埋め込み系列を入力する入力手段と、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と上記埋め込み系列との演算を行うことにより上記電子透かしを解除する演算手段とを有するユーザとを設けている。

【0020】また、本発明による記憶媒体においては、原画像、透かし画像形状情報、及び埋め込み系列を入力する処理と、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する処理とを実行するためのプログラムを記憶している。

【0021】また、本発明による他の記憶媒体においては、電子透かしが埋め込まれた画像、透かし画像形状情報、及び埋め込み系列を入力する処理と、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と、上記埋め込み系列との演算を行うことにより上記電子透かしを解除する処理とを実行するためのプログラムを記憶している。

【0022】さらに、本発明による他の記憶媒体においては、原画像、透かし画像形状情報及び埋め込み系列を入力する処理と、上記透かし画像形状情報により示される形状内に含まれる上記原画像の画素の画素値と、上記埋め込み系列との演算を行うことにより電子透かしが埋め込まれた画像を作成する処理と、上記電子透かしが埋め込まれた画像、上記透かし画像形状情報及び埋め込み系列をユーザに配付する処理と、上記電子透かしが埋め込まれた画像、透かし画像形状情報及び埋め込み系列を入力する処理と、上記透かし画像形状情報により示される形状内に含まれる上記電子透かしが埋め込まれた画像の画素の画素値と上記埋め込み系列との演算を行うことにより上記電子透かしを解除する処理とを実行するためのプログラムを記憶している。

【0023】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。図1は、本発明の第1の実施の形態による電子透かし埋め込み方法の処理を示すフローチャートである。図1において、まず、処理11の初期状態で、画素位置と画素値で構成される複数の画素からなる原画像と、埋め込む画像の形状を示す画素位置からなる透かし画像形状情報と、埋め込み系列としての2進数で表現される所定のシリアルビット系列を設定する。

【0024】次に処理12において、原画像を構成する画素の画素位置と透かし画像形状情報との比較処理を行い、一致したとき、処理13にその画素位置情報を送り、不一致のとき、その画素についての処理を終了する。処理13では、原画像の指定された画素位置の画素値（全部又は一部）と、上記埋め込み系列としての所定のビット（又はビット列）を用いた演算処理を行う。この演算処理としては、排他的論理和やモジュロ加算、モジュロ乗算等の可逆な演算は全て含まれる。

【0025】次に、処理14で埋め込み処理を行い、処理13に送られた画素位置の画素値としての演算結果を出力する。尚、上記の各処理は、各画素毎に順次行うようにしてもよく、また、並列に行うようにしてもよい。

【0026】本実施の形態によれば、原画像に対して透かし画像形状情報を応じた変形を加えることができる。この変形は、前述の不可視型電子透かしと異なり、画素値を処理13の演算結果に応じて大きく変えるので、目に見える可視型透かしとなる。従って、本実施の形態によって生成される画像を、以下の説明では可視型電子透かし埋め込み済み画像と呼ぶものとする。

【0027】上記可視型電子透かし埋め込み済み画像は、次に説明する第2の実施の形態による復号法により復元可能であり、透かし画像形状が著作権者のロゴ等の意味のある情報であれば、単なる画像スクランブルと異なる著作権情報保護の効果を実現することができる。

【0028】図2は、本発明の第2の実施の形態による電子透かし解除方法を示すフローチャートである。図2

10

20

30

30

40

50

において、まず処理21の初期状態で、画素位置と画素値で構成される複数の画素からなる可視型電子透かし埋め込み済み画像と、埋め込む画像の形状を示す画素位置からなる透かし画像形状情報と、第1の実施の形態で埋め込みに用いたものと同じ埋め込み系列としてのシリアルビット系列を設定する。

【0029】次に処理22において、電子透かし埋め込み済み画像を構成する画素の画素位置と透かし画像形状情報との比較処理を行い、一致したとき、処理23にその画素位置情報を送り、不一致のとき、その画素についての処理を終了する。

【0030】処理23では、原画像の指定された画素位置の画素値（全部又は一部）と、埋め込み系列の所定のビット（又はビット列）とを用いた演算処理を行う。ここで、演算処理は透かし埋め込み時に用いられた演算の逆演算である。例えば排他的論理和により、電子透かしが埋め込まれている場合は、再び排他的論理和を演算することによって、原画像の画素の画素値が復元される。処理24では、処理23に送られた画素位置の画素値として演算結果を出力する。尚、上記の各処理は、各画素毎に順次行うようにしてもよく、また、並列に行うようにしてもよい。

【0031】本実施の形態によれば、第1の実施の形態によって生成された可視型電子透かし埋め込み済み画像を原画像に復元することができる。

【0032】図3は、第1の実施の形態の演算処理として暗号処理を用いた場合の本発明の第3の実施の形態による電子透かし埋め込み方法を示すフローチャートである。

【0033】本実施の形態は、処理33以外は、第1の実施の形態の図1と同じである。従って、処理33についてのみ説明する。処理33は、原画像の指定された、画素位置に対して暗号化を行う。この場合、埋め込み系列は暗号鍵又は暗号鍵を生成するための初期値として用いることができる。暗号方式としては、例えばDES（池野、小山、”現代暗号理論”、電子情報通信学会）を用い、各画素値が8bitの値で示される場合、指定された画素位置を8画素位置毎に分割し、その画素値を並べた64bit毎に上記DESによる暗号化を行う。

【0034】このとき、埋め込み系列から所定の56bitを鍵として用いる（さらに、8bitのパリティを付加する）。DESからの出力は入力と同じ64bitであるので、その出力を8bit毎に分割し、各々入力として用いた8つの画素位置の画素値として出力する。

【0035】また、DESをストリーム暗号として用いる場合は、入力系列を鍵、及び初期値として、DESのCBCモードによって疑似乱数を発生させ8bit毎に指定された画素位置の画素値として出力することができる。この場合、発生させる疑似乱数のビット数は指定された画素位置に必要な画素値の数であり、その数になれ

ば終了する。これにより、原画像の復元に必要な大部分の情報は、電子透かし埋め込み済み画像上にあり、画像復元時には、鍵等を表す短いビット列である埋め込み系列を用いればよい埋め込み方法が実現される。

【0036】図4は、上記第3の実施の形態によって埋め込まれた電子透かしを解除するための、本発明の第4の実施の形態による電子透かし解除方法を示すフローチャートである。本実施の形態は、処理43以外は、第3の実施の形態の図3と同じである。従って、処理33についてのみ説明する。処理43は、電子透かし埋め込み済み画像の指定された画素位置に対して復号を行う。この場合、埋め込み系列は、埋め込みに用いた暗号鍵に対応する復号鍵又は復号鍵を生成するための初期値として用いることができる。

【0037】本実施の形態によれば、DESからの出力を透かし埋め込み時と同じ画素位置で8bit毎に分割し出力する。これにより、図3の電子透かし埋め込み方法により埋め込まれた電子透かしの解除を行うことができる。

【0038】本実施の形態では、暗号化方式としてDESを例に挙げたが、他の共通鍵暗号方式、例えば、FEAL、IDEA、RC2、RC4、RC5、MISTY、シーザー型暗号、ビジネル暗号・ビューフォート暗号、ブレイフェア暗号、ヒル暗号、バーナム暗号等を用いることもできる。

【0039】図5は本発明の第5の実施の形態を示すもので、第1の実施の形態の電子透かし埋め込み方法を用いて構成した電子透かし埋め込み装置及び第2の実施の形態の電子透かし解除方式を用い構成した電子透かし解除装置を使用したネットワークによるデジタル画像配布システムを示すものである。本システムは、原画像に電子透かしを埋め込みユーザに供給するサーバ51と、画像をサーバより購入するユーザ52と、サーバ51とユーザ52の間で情報の交換を行うインターネットに代表される配布手段58とからなる。

【0040】サーバ51は、原画像、電子透かし埋め込み済み画像、透かし画像形状情報及び埋め込み系列を保存しておく記憶装置53と、第1の実施の形態の電子透かし埋め込み方法を用いて構成した電子透かし埋め込み装置54とからなる。

【0041】ユーザ52は、取得した電子透かし埋め込み済み画像、透かし画像形状情報、入力系列及び電子透かしを解除した画像を保存する記憶装置55と、第2の実施の形態の電子透かし解除方法を用いて構成した電子透かし解除装置56と、画像表示装置57とからなる。

【0042】サーバ51である画像販売者は、記憶装置53に原画像、透かし画像形状情報、及び埋め込み系列を保持している。それらのデータを電子透かし埋め込み装置54に入力して電子透かし埋め込み済み画像を得、記憶装置53に保存する。透かし画像形状は、例えば著

作者を表すロゴの形状をしているものとする。この場合、埋め込み系列は、各々のユーザ（画像購入者）に固有である場合、共通である場合、その他ユーザ、サーバ、画像によって様々な場合が考えられる。

【0043】電子透かしの不正解除を妨げるため、ユーザ同士の埋め込み系列の交換、譲渡を防ぎ、またある画像の埋め込み系列により他の画像の電子透かしを解除することを防ぐため、同じ埋め込み系列で電子透かしを埋め込んだ数種類の画像を比較することにより埋め込み系列が割り出されることを防ぐため等の理由から、配布を行うたびに埋め込み系列を生成すること、つまり、全ての配布画像毎に埋め込み系列を変えることがサーバにとって有利である。

【0044】電子透かし埋め込み済み画像は、ユーザ52からの要求によって配布手段58により配布され、ユーザ52の記憶装置55に保存される。ユーザ52は、保存した画像を画像表示装置57で確認し、必要であれば、サーバ51と契約及び／又は料金の支払い等の必要な手続きを行う。

【0045】手続き終了後、サーバ51は、記憶装置53に保存してある透かし画像形状情報、埋め込み系列を配布手段58を通じてユーザ52に配布する。ユーザ52は、一旦記憶装置55に保存した後、電子透かし埋め込み済み画像と共に電子透かし解除装置56に入力して原画像を復元する。

【0046】本実施の形態では、一般的な方法として埋め込み情報配布前に契約等手続きを行う旨述べたが、透かし埋め込み済み画像の配布時等、他のタイミングにおいても手続きが行われる場合も考えられる。また、課金方法としては、電子マネー等のネットワーク上で行うものの他に、クレジットカード及び現金等の一般的なものも可能である。また、電子透かしを埋め込まれた画像や埋め込み系列等、通信路上に送信されるデータは、一般的な通信路暗号化方式により暗号化されて送信される場合もある。

【0047】図6は、本発明の第6の実施の形態を示すもので、第3の実施の形態の電子透かし埋め込み方法を用いて構成した電子透かし埋め込み装置の暗号化装置及び電子透かし解除装置の復号装置に、RSA等の公開鍵暗号方式を用いて構成したネットワークによるデジタル画像配布システムを示すものである。本システムにおいては、デジタル画像が配布される以前に、印刷物、記録媒体、ネットワーク、口頭、その他の方法で契約及び／又は課金が行われているものとする。

【0048】図6において、上記第5の実施の形態でサーバが埋め込み系列（共通鍵）を保有していたのと異なり、ユーザ63が鍵生成部69で公開鍵と秘密鍵の対を作成する。公開鍵は、ネットワークを通して、認証局62の公開鍵記憶装置66に、秘密鍵はユーザ63が保有する記憶装置68に各々保存される。

【0049】サーバ61は、ユーザ63との契約に従って、認証局62の公開鍵記憶装置66よりユーザ63の公開鍵を取り出し、これを埋め込み系列の一部或いは全部とし、記憶装置64の原画像、透かし形状情報と共に電子透かし埋め込み装置65に入力し、電子透かし埋め込み済み画像を得て、記憶装置64に一時保存する。この画像は配布手段71を通じてユーザ63に配布され、記憶装置60に保存してある秘密鍵を一部或いは全部とする系列と共に、電子透かし解除装置58に入力され、電子透かしが解除される。

【0050】ユーザの公開鍵を用いて電子透かしを埋め込んだ画像をユーザに配布することにより、このユーザの持つ秘密鍵を用いなければ透かし画像を取り除くことはできない。また、秘密鍵はインターネット上に送信されず、ユーザ63のローカルな環境のみに存在するので、インターネット上に多数存在する悪意の攻撃者に電子透かしの入っていない画像が渡ることを防ぐ効果がある。

【0051】また、暗号化を原画像全体に行う方法に比べて暗号化及び復号に必要な時間が短くなる。また、上記第4の実施の形態の電子透かし埋め込み方式と組み合わせ、二重或いは部分毎に共通鍵暗号方式と公開鍵暗号方式による電子透かしを埋め込むという方式も考えられる。

【0052】図7は、本発明の第7の実施の形態を示すもので、原画像に不可視の電子透かしを埋め込み、さらに、第1の実施の形態の電子透かし埋め込み方法を用いて構成した装置により、可視の電子透かしを埋め込むようにしたを特徴とした画像配布システムを示すものである。

【0053】本システムは、原画像に電子透かしを埋め込みユーザに供給するサーバ81、画像をサーバより購入するユーザ82、原画像、電子透かし埋め込み済み画像、透かし画像形状情報及び埋め込み系列を保存しておく記憶装置83、不可視型電子透かしを埋め込む不可視透かし埋め込み装置84、第1の実施の形態の電子透かし埋め込み方法を用いて構成した可視透かし埋め込み装置85を有する。

【0054】さらに、取得した電子透かし埋め込み済み画像、透かし画像形状情報、埋め込み系列、電子透かしを解除した画像を保存する記憶装置86、第3の実施の形態の方法を用いて構成した電子透かし解除装置87、画像表示装置88、サーバ81とユーザ82の間で情報の交換を行うインターネットに代表される配布手段89を有する。

【0055】サーバ81である画像販売者は、記録装置83に原画像、透かし画像形状情報、可視透かしとして埋め込む埋め込み系列、及び不可視透可視として埋め込む情報を保持している。原画像と不可視透かしとして埋め込む情報を不可視透かし埋め込み装置84に入力し、

不可視透かし埋め込み済み画像を得る。不可視の透かし埋め込み済み画像は見た目には原画像と全く同じである。

【0056】不可視透かし埋め込み済み画像は、記憶装置83に保持している透かし画像形状情報、埋め込み系列と共に可視透かし埋め込み装置85に入力され、不可視及び可視透かし埋め込み済み画像が outputされ、記憶装置83に保存される。尚、ユーザ側の処理については、第4の実施の形態と同様であるので説明を省略する。

【0057】ユーザ側で可視透かしを取り除いた画像は原画像と見た目には同一なので、原画像と同等に利用できる。見た目には同一であるが不可視透かしとして埋め込まれた情報は残っているので、情報を抽出する装置を用いることにより、不可視透かしとして埋め込まれた埋め込み情報を抽出し利用することができる。不正使用された画像が発見されたときに、サーバ或いは警察機関等が情報を抽出するのが一般的と考えられる。

【0058】これによって、不正再配布、不正使用等を十分防ぐことができ、かつ可視電子透かしの正式あるいは不正解除後も、不可視の電子透可視により埋め込まれている情報により一定レベルのセキュリティを保つことができる画像配布システムを実現できる。

【0059】次に本発明の他の実施の形態としての記憶媒体について説明する。本発明の目的は、ハードウェア構成により達成することも可能であり、また、CPUとメモリとで構成されるコンピュータシステムで達成することもできる。本発明をコンピュータシステムで構成する場合、上記メモリは本発明による記憶媒体を構成する。

【0060】即ち、上述した各実施の形態において説明した図1～図4のフローチャートによる動作を実行するためのソフトウェアのプログラムコードを記憶した記憶媒体をシステムや装置で用い、そのシステムや装置のCPUが上記記憶媒体に格納されたプログラムコードを読み出し、実行することにより、本発明の目的を達成することができる。

【0061】また、この記憶媒体としては、ROM、RAM等の半導体メモリ、光ディスク、光磁気ディスク、磁気媒体等を用いてよく、これらをCD-ROM、フロッピディスク、磁気媒体、磁気カード、不揮発性メモリカード等に構成して用いてよい。

【0062】従って、この記憶媒体を図5～図7に示したシステムや装置以外の他のシステムや装置で用い、そのシステムあるいはコンピュータがこの記憶媒体に格納されたプログラムコードを読み出し、実行することによっても、前述した各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0063】また、コンピュータ上で稼働しているOS等が処理の一部又は全部を行う場合、あるいは記憶媒体

から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された拡張機能ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づいて、上記拡張機能ボードや拡張機能ユニットに備わるCPU等が処理の一部又は全部を行う場合にも、各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0064】

【発明の効果】以上説明したように、本発明によれば、原画像、透かし画像形状情報、及び埋め込み系列を入力とし、透かし画像形状情報によって示される透かし画像の形状内に含まれる原画像の画素の画素値と、埋め込み系列との演算を行うことにより、セキュリティの高い可視型電子透かしを原画像に埋め込むことができ、著作権の保護を十分に行うことができる。

【0065】また、電子透かしが埋め込まれた画像と透かし形状情報を上記と逆演算することにより、電子透かしを解除して原画像を復元することができる。

【0066】さらに、可視型電子透かしが埋め込まれた画像を作成して、配付するシステムを実現することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態による電子透かし埋め込み方法を示すフローチャートである。

【図2】本発明の第2の実施の形態による電子透かし解除方法を示すフローチャートである。

【図3】本発明の第3の実施の形態による電子透かし埋*

*め込み方法を示すフローチャートである。

【図4】本発明の第4の実施の形態による電子透かし解除方法を示すフローチャートである。

【図5】本発明の第5の実施の形態による上記電子透かし埋め込み方法を用いたネットワークによるデジタル画像配布システムのブロック図である。

【図6】本発明の第6の実施の形態による上記電子透かし埋め込み方法を用いたネットワークによるデジタル画像配布システムのブロック図である。

【図7】本発明の第6の実施の形態による可視型電子透かしと不可視型電子透かしを埋め込むようにしたネットワークによるデジタル画像配布システムのブロック図である。

【符号の説明】

51、61、81 サーバ

52、63、82 ユーザ

53、55、64、68、83 記憶装置

54、65 電子透かし埋め込み装置

56、70 電子透かし解除装置

57、67、88 画像表示装置

58、71、89 配付手段

62 認証局

66 公開鍵記憶装置

69 鍵生成部

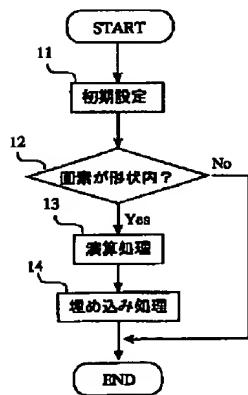
84 不可視透かし埋め込み装置

85 可視透かし埋め込み装置

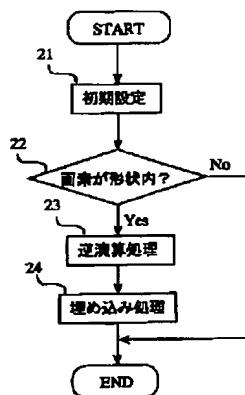
86 画像記憶装置

87 可視透かし解除装置

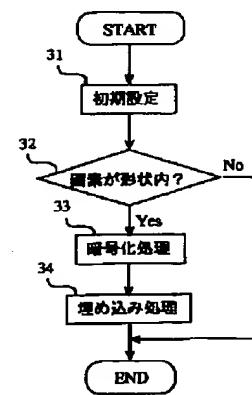
【図1】



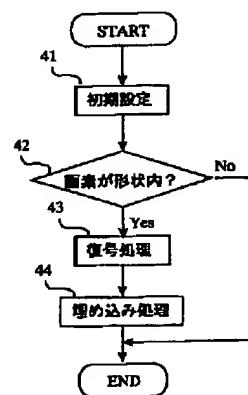
【図2】



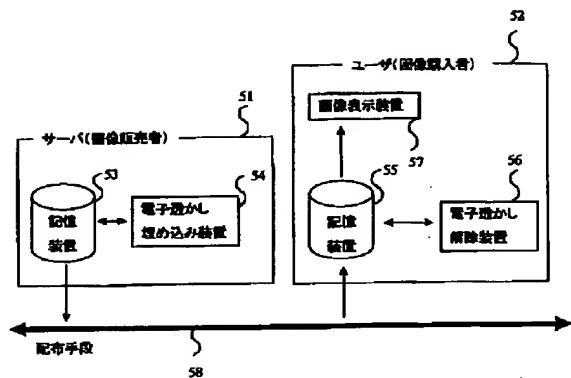
【図3】



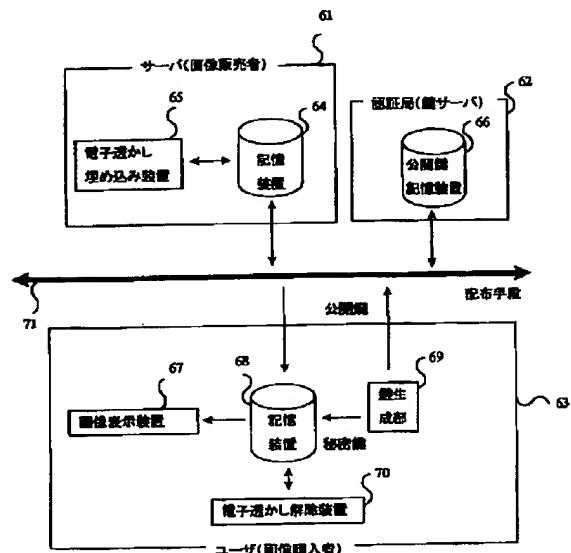
【図4】



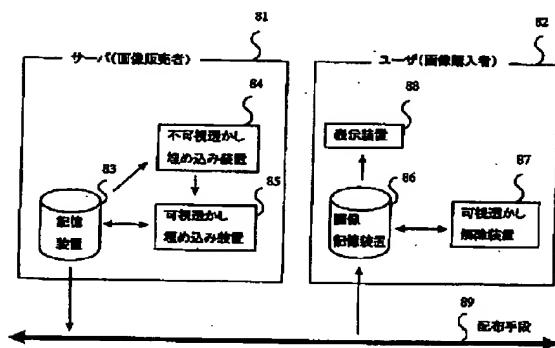
【図5】



【図6】



【図7】



フロントページの続き

F ターム(参考) 5B057 AA20 CA20 CB20 CC01 CE20
 DA20 DC31
 5C075 AB00 EE02 EE03
 5C076 AA14
 5J104 AA07 AA14 EA19 JA03 JA21
 KA01 MA01 PA14